LAPORAN PRAKTIKUM KEAMANAN SIBER (TEK1314)

MINGGU 2: WINDOWS INFRASTRUCTURE DEFENDER

KELOMPOK: 1 | KELAS: TEK-G1

HOSTNAME PC/VM: CAKOM1-14

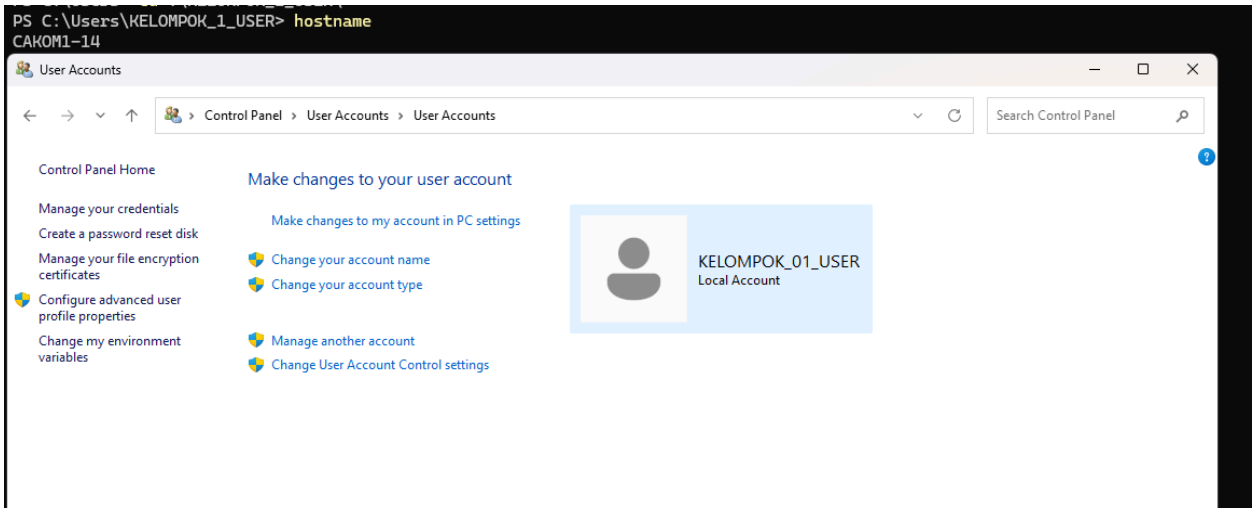
Daftar Anggota & Pembagian Peran (PBL)

No	Nama / NIM	Peran (Role)	Tanggung Jawab Utama
1	RADYANKA IRZA PRAMONO | J0404231110	Technical Writer (Lead)	Konsolidasi screenshot, narasi laporan, & cek integritas.
2	Iqbaal Maulana Dwiputera / J0404231082	Identity & Shell Auditor	Lab 3.3.10 (User) & 3.3.11 (PowerShell/Netstat).
3	Ahmad Farrell Raafii Alaiyya Al attas J0404231031	System Analyst	Lab 3.2.11 (Registry) & 3.0.3 (Process Explorer).
4	Gesit Tri Nugroho | J0404231025	Resource Monitor	Lab 3.3.12 (Task Manager) & 3.3.13 (Perf Monitor).

FASE 1: IDENTITY & SHELL AUDIT (PIC: Anggota 2)

Referensi: Lab 3.3.10 & 3.3.11

1. Bukti Akun User Baru:



2. Hasil Audit Jaringan (PowerShell):
   - Perintah yang digunakan: netstat -ano
   - PID Terdeteksi (Established): 19720

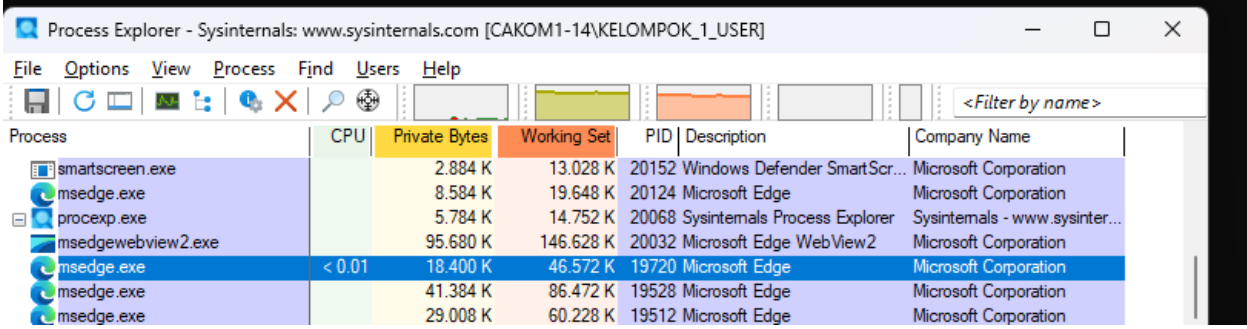
```
PS C:\Users\KELOMPOK_1_USER> hostname
CAKOM1-14
PS C:\Users\KELOMPOK_1_USER> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1428
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
```

```
  TCP    172.22.6.125:50083     172.17.11.13:53        TIME_WAIT       0
  TCP    172.22.6.125:50108     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50128     150.171.22.17:443      TIME_WAIT       0
  TCP    172.22.6.125:50129     172.22.6.160:7680      TIME_WAIT       0
  TCP    172.22.6.125:50130     52.110.20.225:443      ESTABLISHED     25644
  TCP    172.22.6.125:50131     52.109.124.141:443     ESTABLISHED     25644
  TCP    172.22.6.125:50399     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50400     23.38.195.144:443      ESTABLISHED     26280
  TCP    172.22.6.125:50414     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50542     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50618     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50688     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50835     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50901     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50928     172.17.9.25:53         TIME_WAIT       0
  TCP    172.22.6.125:50978     170.72.253.46:443      ESTABLISHED     9800
  TCP    172.22.6.125:51051     23.38.195.138:443      ESTABLISHED     19720
  TCP    172.22.6.125:51116     172.17.9.25:53         TIME_WAIT       0
```

```
PS C:\Users\KELOMPOK_1_USER> hostname
CAKOM1-14
```

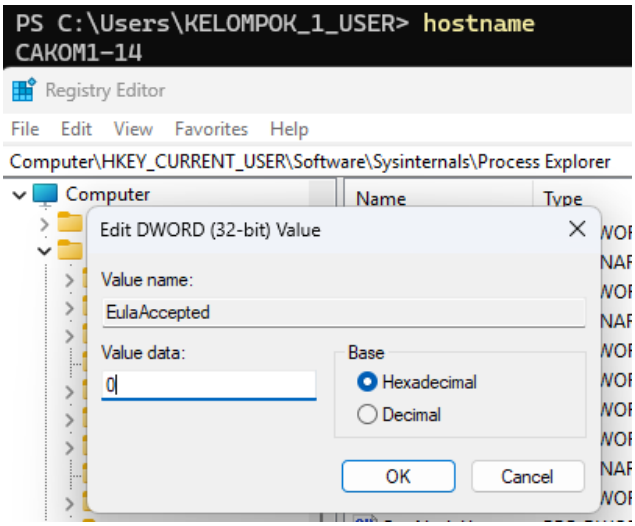


3. Analisis Auditor: Mengapa prinsip *Least Privilege* (Standard User) krusial dalam pertahanan infrastruktur web?
    - Jawaban: Prinsip *Least Privilege* krusial dalam pertahanan infrastruktur karena membatasi dampak kerusakan (*blast radius*) dengan memastikan setiap pengguna, termasuk analis, hanya beroperasi dengan hak akses minimal yang diperlukan (Standard User) daripada Administrator untuk aktivitas harian . Penerapan ini vital karena jika akun analis terkompromi oleh *malware* atau serangan siber, penyerang tidak dapat langsung mematikan kontrol keamanan, mengubah konfigurasi sistem inti, atau menginstal *rootkit* secara global, sehingga isolasi ancaman menjadi lebih efektif dan mencegah eskalasi hak akses yang dapat melumpuhkan seluruh jaringan.

FASE 2: DEEP PROCESS & REGISTRY ANALYSIS (PIC: Anggota 3)

Referensi: Lab 3.2.11 & 3.0.3

1. Analisis PID Target (dari Fase 1):
    - Nama Proses: msedge.exe
    - Path File: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
2. Verifikasi Keamanan: Apakah proses ini termasuk *Windows Process* yang valid atau mencurigakan? Jelaskan alasannya.
    - Jawaban: Proses ini adalah eksekusi resmi milik aplikasi Microsoft Edge, sehingga termasuk proses yang valid dan bukan malware. Jika file berada di temp atau lokasi yang mencurigakan, barulah kita harus waspada..
3. Audit Manipulasi Registri:
    - Screenshot bukti perubahan EulaAccepted (0 -> 1):

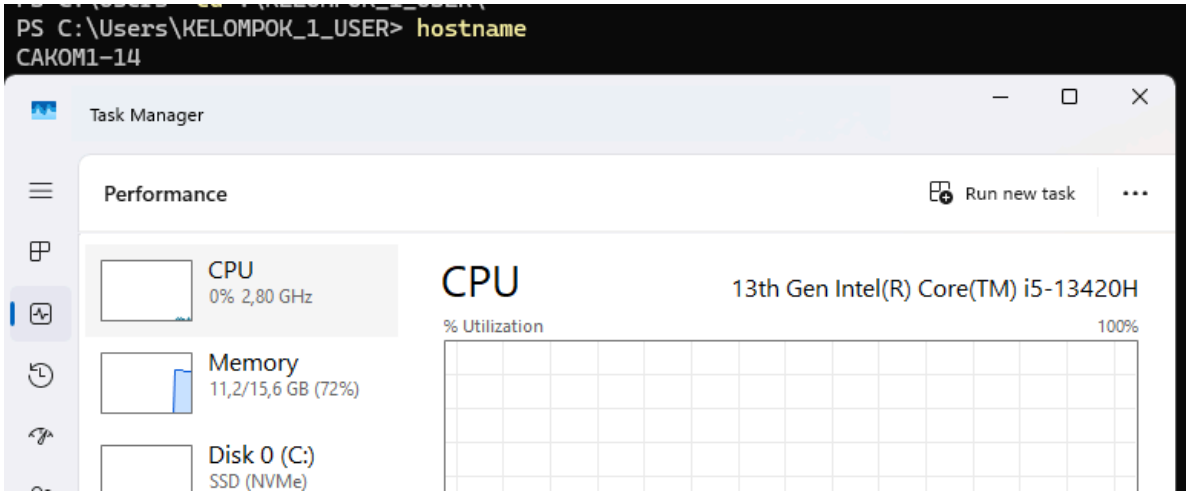


    - Analisis: Bagaimana *attacker* memanfaatkan Registry untuk *Persistence* (bertahan di sistem)?
    - Jawaban: Penyerang (attacker) sering memanipulasi Windows Registry untuk mencapai persistence agar malware dapat dieksekusi secara otomatis setiap kali sistem dinyalakan (booting) atau pengguna melakukan login, sehingga akses ilegal tetap terjaga meskipun komputer telah dimatikan atau di-restart. Dengan menyisipkan lokasi file berbahaya ke dalam kunci registri otoritatif seperti Run atau RunOnce, penyerang dapat menyembunyikan mekanisme startup mereka di lokasi yang jarang diperiksa oleh pengguna biasa (stealth), menjadikannya lebih sulit dideteksi dan dibersihkan dibandingkan jika hanya menaruh file di folder Startup konvensional.

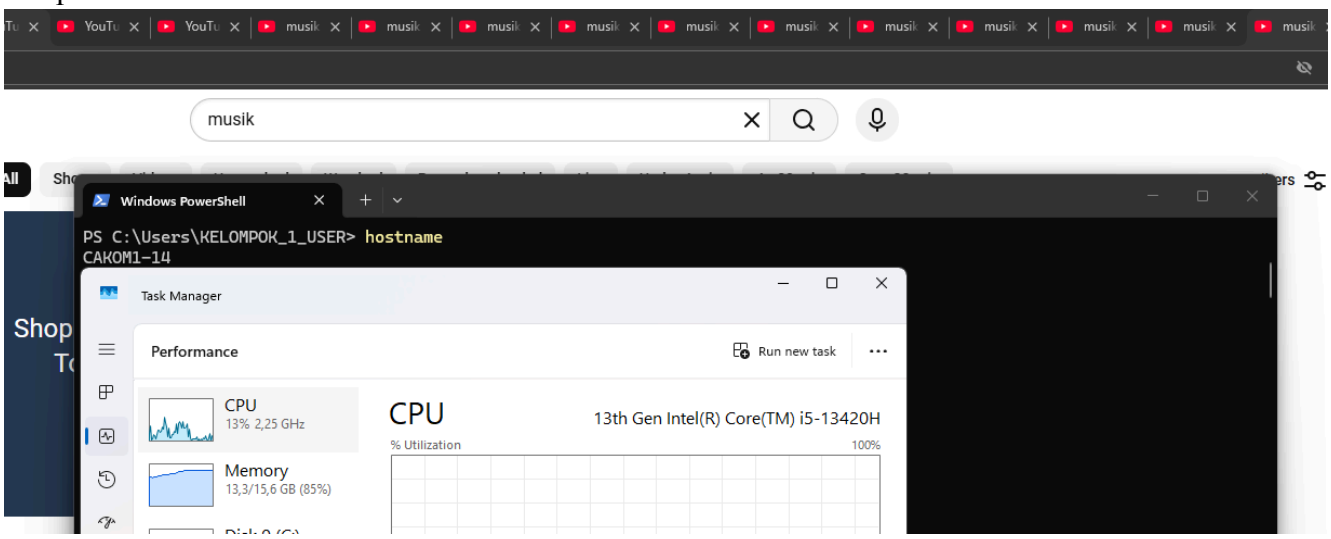
FASE 3: RESOURCE BASELINE MONITORING (PIC: Anggota 4)

Referensi: Lab 3.3.12 & 3.3.13

1. Screenshot Performance Monitor (Load Test):
   Tampilan saat Idle:



   Tampilan saat membuka 10 Halaman Web:



2. Tabel Baseline Kelompok:

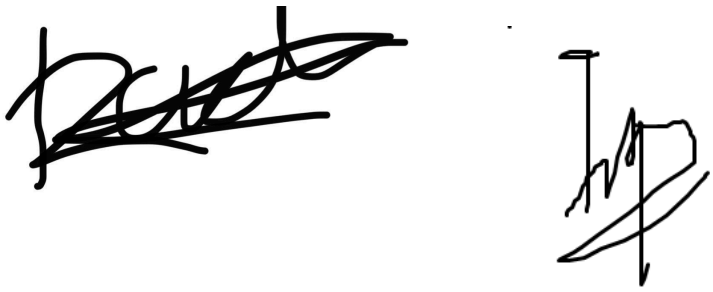
Indikator	Hasil Idle (Normal)	Hasil Load (Sibuk)
CPU	0%	13%
RAM Available	4.4 GB	2.3 GB

3. Analisis Monitor: Mengapa seorang analis SOC harus mengetahui angka *Idle* (diam) pada sebuah server?
    - Jawaban: Analisis SOC wajib mengetahui angka baseline (Idle) untuk memahami kondisi saat normal, untuk mendeteksi anomali atau serangan, jika sebuah server dalam kondisi Idle biasanya menggunakan CPU sebesar 6%, secara tiba tiba naik ke 95% tanpa ada aktivitas oleh user yang sah. Ini merupakan sebuah indikator adanya aktivitas tidak wajar seperti serangan DDoS atau proses lain yang tidak sah.

FASE 4: KONSOLIDASI & KESIMPULAN (PIC: Technical Writer/Lead)

Review oleh seluruh anggota kelompok

1. Korelasi Temuan: Apakah proses yang memakan CPU tinggi di Fase 3 berkorelasi dengan PID yang ditemukan di Fase 1? Jelaskan.
    - Jawaban: PID 19720 yang diidentifikasi pada Fase 1 dan 2 adalah msedge.exe, yang merupakan proses dari aplikasi Microsoft Edge untuk merender konten web. pada Fase 3 sistem dicoba untuk menjalankan 10 halaman web youtube secara bersamaan. Lonjakan CPU dan RAM pada performance monitor disebabkan oleh aktivitas thread dan penggunaan memori dari PID 19720 tersebut beserta proses child lainnya. Hal ini membuktikan bahwa aktivitas user dalam penggunaan aplikasi secara langsung memengaruhi profil resource baseline sistem yang sedang diaudit.
2. Pernyataan Integritas: Kami menyatakan laporan ini dibuat secara kolaboratif sesuai Kontrak Kuliah poin 5.
    - Tanda Tangan Digital/Nama Terang Anggota:
      (1) RADYANKA IRZA PRAMONO (2) Iqbaal Maulana Dwiputera



    - (3) Ahmad Farrell Raafii Alaiyya Al attas (4) Gesit Tri Nugroho